TITLE VIII--ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS

SUBTITLE B--INFORMATION TECHNOLOGY

SEC. 811. ACQUISITION AND MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) Responsibility of DOD Chief Information Officer Relating to Mission Critical and Mission Essential Information Technology Systems.--Section 2223(a) of title 10, United States Code, is amended--

(1) by striking ``and'' at the end of paragraph (3);

(2) by striking the period at the end of paragraph (4) and inserting ``; and''; and

(3) by adding at the end the following:

``(5) maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.''.

(b) Minimum Planning Requirements for the Acquisition of Information Technology Systems.--(1) Not later than 60 days after the date of the enactment of this Act, Department of Defense Directive 5000.1 shall be revised to establish minimum planning requirements for the acquisition of information technology systems.

(2) The revised directive required by (1) shall--

(A) include definitions of the terms ``mission critical information system'' and ``mission essential information system'';

(B) prohibit the award of any contract for the acquisition of a mission critical or mission essential information technology system until--

(i) the system has been registered with the Chief Information Officer of the Department of Defense;

(ii) the Chief Information Officer has received all information on the system that is required under the directive to be provided to that official; and

(iii) the Chief Information Officer has determined that there is in place for the system an appropriate information assurance strategy; and

(C) require that, in the case of each system registered pursuant to subparagraph (B)(i), the information required under subparagraph (B)(ii) to be submitted as part of the registration shall be updated on not less than a quarterly basis.

(c) Milestone Approval for Major Automated Information Systems.--The revised directive required by subsection (b) shall prohibit Milestone I approval, Milestone II approval, or Milestone III approval (or the equivalent) of a major automated information system within the Department of Defense until the Chief Information Officer has determined that--

(1) the system is being developed in accordance with the requirements of division E of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

(2) appropriate actions have been taken with respect to the system in the areas of business process reengineering, analysis of alternatives, economic analysis, and performance measures; and

(3) the system has been registered as described in subsection (b)(2)(B).

(d) Notice of Redesignation of Systems.--(1) Whenever during fiscal year 2001, 2002, or 2003 the Chief Information Officer designates a system previously designated as a major automated information system to be in a designation category other than a major automated information system, the Chief Information Officer shall notify the congressional defense committees of that designation. The notice shall be provided not later than 30 days after the date of that designation. Any such notice shall include the rationale for the decision to make the designation and a description of the program management oversight that will be implemented for the system so designated.

(2) Not later than 60 days after the date of the enactment of this Act, the Chief Information Officer shall submit to the congressional defense committees a report specifying each information system of the Department of Defense previously designated as a major automated information system that is currently designated in a designation category other than a major automated information system including designation as a ``special interest major technology initiative''. The report shall include for each such system the information specified in the third sentence of paragraph (1).

(e) Annual Implementation Report.--(1) The Secretary of Defense shall submit to the congressional defense committees, not later than April 1 of each of fiscal years 2001, 2002, and 2003, a report on the implementation of the requirements of this section during the preceding fiscal year.

(2) The report for a fiscal year under paragraph (1) shall include, at a minimum, for each major automated information system that was approved during such preceding fiscal year under Department of Defense Directive 5000.1 (as revised pursuant to subsection (b)), the following:

(A) The funding baseline.

(B) The milestone schedule.

(C) The actions that have been taken to ensure compliance with the requirements of this section and the directive.

(3) The first report shall include, in addition to the information required by paragraph (2), an explanation of the manner in which the responsible officials within the Department of Defense have addressed, or intend to address, the following acquisition issues for each major automated information system planned to be acquired after that fiscal year:

(A) Requirements definition.

(B) Presentation of a business case analysis, including an analysis of alternatives and a calculation of return on investment.

(C) Performance measurement.

(D) Test and evaluation.

(E) Interoperability.

(F) Cost, schedule, and performance baselines.

(G) Information assurance.

(H) Incremental fielding and implementation.

(I) Risk mitigation.

(J) The role of integrated product teams.

(K) Issues arising from implementation of the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Plan required by Department of Defense Directive 5000.1 and Chairman of the Joint Chiefs of Staff Instruction 3170.01.

(L) Oversight, including the Chief Information Officer's oversight of decision reviews.

(f) Definitions.--In this section:

(1) The term ``Chief Information Officer'' means the senior official of the Department of Defense designated by the Secretary of Defense pursuant to section 3506 of title 44, United States Code.

(2) The term ``information technology system'' has the meaning given the term ``information technology'' in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

(3) The term ``major automated information system'' has the meaning given that term in Department of Defense Directive 5000.1.

SEC. 812. TRACKING AND MANAGEMENT OF INFORMATION TECHNOLOGY PURCHASES.

(a) In General.--(1) Chapter 131 of title 10, United States Code, is amended by adding at the end the following new section:

``2225. Information technology purchases: tracking and management

``(a) Collection of Data Required.--To improve tracking and management of information technology products and services by the Department of Defense, the Secretary of Defense shall provide for the collection of the data described in subsection (b) for each purchase of such products or services made by a military department or Defense Agency in excess of the simplified acquisition threshold, regardless of whether such a purchase is made in the form of a contract, task order, delivery order, military interdepartmental purchase request, or any other form of interagency agreement.

``(b) Data To Be Collected.--The data required to be collected under subsection (a) includes the following:

``(1) The products or services purchased.

``(2) Whether the products or services are categorized as commercially available off-the-shelf items, other commercial items, nondevelopmental items other than commercial items, other noncommercial items, or services.

``(3) The total dollar amount of the purchase.

``(4) The form of contracting action used to make the purchase.

``(5) In the case of a purchase made through an agency other than the Department of Defense--

``(A) the agency through which the purchase is made; and

``(B) the reasons for making the purchase through that agency.

``(6) The type of pricing used to make the purchase (whether fixed price or another type of pricing).

``(7) The extent of competition provided in making the purchase.

``(8) A statement regarding whether the purchase was made from--

``(A) a small business concern;

``(B) a small business concern owned and controlled by socially and economically disadvantaged individuals; or

``(C) a small business concern owned and controlled by women.

``(9) A statement regarding whether the purchase was made in compliance with the planning requirements under sections 5122 and 5123 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1422, 1423).

``(c) Responsibility To Ensure Fairness of Certain Prices.--The head of each contracting activity in the Department of Defense shall have responsibility for ensuring the fairness and reasonableness of unit prices paid by the contracting activity for information technology products and services that are frequently purchased commercially available off-the-shelf items.

``(d) Limitation on Certain Purchases.--No purchase of information technology products or services in excess of the simplified acquisition threshold shall be made for the Department of Defense from a Federal agency outside the Department of Defense unless--

``(1) the purchase data is collected in accordance with subsection (a); or

``(2)(A) in the case of a purchase by a Defense Agency, the purchase is approved by the Under Secretary of Defense for Acquisition, Technology, and Logistics; or

``(B) in the case of a purchase by a military department, the purchase is approved by the senior procurement executive of the military department.

``(e) Annual Report.--Not later than March 15 of each year, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report containing a summary of the data collected in accordance with subsection (a).

``(f) Definitions.--In this section:

``(1) The term `senior procurement executive', with respect to a military department, means the official designated as the senior procurement executive for the military department for the purposes of section 16(3) of the Office of Federal Procurement Policy Act (41 U.S.C. 414(3)).

``(2) The term `simplified acquisition threshold' has the meaning given the term in section 4(11) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(11)).

``(3) The term `small business concern' means a business concern that meets the applicable size standards prescribed pursuant to section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

``(4) The term `small business concern owned and controlled by socially and economically disadvantaged individuals' has the meaning

given that term in section 8(d)(3)(C) of the Small Business Act (15 U.S.C. 637(d)(3)(C)).

``(5) The term `small business concern owned and controlled by women' has the meaning given that term in section 8(d)(3)(D) of the Small Business Act (15 U.S.C. 637(d)(3)(D)).".

(2) The table of sections at the beginning of such chapter is amended by adding at the end the following:

``2225. Information technology purchases: tracking and management.".

(b) Time for Implementation; Applicability.--(1) The Secretary of Defense shall collect data as required under section 2225 of title 10, United States Code (as added by subsection (a)) for all contractual actions covered by such section entered into on or after the date that is one year after the date of the enactment of this Act.

(2) Subsection (d) of such section shall apply with respect to purchases described in that subsection for which solicitations of offers are issued on or after the date that is one year after the date of the enactment of this Act.

(c) GAO Report.--Not later than 15 months after the date of the enactment of this Act, the Comptroller General shall submit to the congressional defense committees a report on the collection of data under such section 2225. The report shall include the Comptroller General's assessment of the extent to which the collection of data meets the requirements of that section.

SEC. 813. APPROPRIATE USE OF REQUIREMENTS REGARDING EXPERIENCE AND EDUCATION OF CONTRACTOR PERSONNEL IN THE PROCUREMENT OF INFORMATION TECHNOLOGY SERVICES.

(a) Amendment of the Federal Acquisition Regulation.--Not later than 180 days after the date of the enactment of this Act, the Federal Acquisition Regulation issued in accordance with sections 6 and 25 of the Office of Federal Procurement Policy Act (41 U.S.C. 405 and 421) shall be amended to address the use, in the procurement of information technology services, of requirements regarding the experience and education of contractor personnel.

(b) Content of Amendment.--The amendment issued pursuant to subsection (a) shall, at a minimum, provide that solicitations for the procurement of information technology services shall not set forth any minimum experience or educational requirement for proposed contractor personnel in order for a bidder to be eligible for award of a contract unless--

(1) the contracting officer first determines that the needs of the executive agency cannot be met without any such requirement; or

(2) the needs of the executive agency require the use of a type of contract other than a performance-based contract.

(c) GAO Report.--Not later than one year after the date on which the regulations required by subsection (a) are published in the Federal Register, the Comptroller General shall submit to Congress an evaluation of--

(1) executive agency compliance with the regulations; and

(2) conformance of the regulations with existing law, together with any recommendations that the Comptroller General considers appropriate.

(d) Definitions.--In this section:

(1) The term ``executive agency'' has the meaning given that term in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

(2) The term ``information technology'' has the meaning given that term in section 5002(3) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)).

(3) The term ``performance-based'', with respect to a contract, means that the contract includes the use of performance work statements that set forth contract requirements in clear, specific, and objective terms with measurable outcomes.

TITLE X--GENERAL PROVISIONS

SUBTITLE F--MISCELLANEOUS REPORTING REQUIREMENTS

SEC. 1053. REPORT ON FEDERAL GOVERNMENT PROGRESS IN DEVELOPING INFORMATION ASSURANCE STRATEGIES.

Not later than January 15, 2001, the President shall submit to Congress a comprehensive report detailing the specific steps taken by the Federal Government as of the date of the report to develop critical infrastructure assurance strategies as outlined by Presidential Decision Directive No. 63 (PDD 63). The report shall include the following:

(1) A detailed summary of the progress of each Federal agency in developing an internal information assurance plan.

(2) The progress of Federal agencies in establishing partnerships with relevant private sector industries to address critical infrastructure vulnerabilities.

SUBTITLE G--GOVERNMENT INFORMATION SECURITY REFORM

SEC. 1061. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by inserting at the end the following new subchapter:

``SUBCHAPTER II--INFORMATION SECURITY

``3531. Purposes

``The purposes of this subchapter are the following:

``(1) To provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets.

``(2)(A) To recognize the highly networked nature of the Federal computing environment including the need for Federal Government interoperability and, in the implementation of improved security management measures, assure that opportunities for interoperability are

not adversely affected.
``(B) To provide effective Government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities.
``(3) To provide for development and maintenance of minimum controls required to protect Federal information and information systems.
``(4) To provide a mechanism for improved oversight of Federal agency information security programs.
``3532. Definitions

``(a) Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.
``(b) In this subchapter:

``(1) The term `information technology' has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).
``(2) The term `mission critical system' means any telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that--
``(A) is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);
``(B) is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy; or
``(C) processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.
``3533. Authority and functions of the Director

``(a)(1) The Director shall establish Government-wide policies for the management of programs that--
``(A) support the cost-effective security of Federal information systems by promoting security as an integral component of each agency's business operations; and
``(B) include information technology architectures as defined under section 5125 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1425).
``(2) Policies under this subsection shall--

``(A) be founded on a continuing risk management cycle that recognizes the need to--
``(i) identify, assess, and understand risk; and

``(ii) determine security needs commensurate with the level of risk;

``(B) implement controls that adequately address the risk;

``(C) promote continuing awareness of information security risk; and

``(D) continually monitor and evaluate policy and control effectiveness of information security practices.
``(b) The authority under subsection (a) includes the authority to--

``(1) oversee and develop policies, principles, standards, and

guidelines for the handling of Federal information and information resources to improve the efficiency and effectiveness of governmental operations, including principles, policies, and guidelines for the implementation of agency responsibilities under applicable law for ensuring the privacy, confidentiality, and security of Federal information;

``(2) consistent with the standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100 235; 101 Stat. 1729), require Federal agencies to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency;

``(3) direct the heads of agencies to--

``(A) identify, use, and share best security practices;

``(B) develop an agency-wide information security plan;

``(C) incorporate information security principles and practices throughout the life cycles of the agency's information systems; and

``(D) ensure that the agency's information security plan is practiced throughout all life cycles of the agency's information systems;

``(4) oversee the development and implementation of standards and guidelines relating to security controls for Federal computer systems by the Secretary of Commerce through the National Institute of Standards and Technology under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g 3);

``(5) oversee and coordinate compliance with this section in a manner consistent with--

``(A) sections 552 and 552a of title 5;

``(B) sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g 3 and 278g 4);

``(C) section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

``(D) sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100 235; 101 Stat. 1729); and

``(E) related information management laws; and

``(6) take any authorized action under section 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) that the Director considers appropriate, including any action involving the budgetary process or appropriations management process, to enforce accountability of the head of an agency for information resources management, including the requirements of this subchapter, and for the investments made by the agency in information technology, including--

``(A) recommending a reduction or an increase in any amount for information resources that the head of the agency proposes for the budget submitted to Congress under section 1105(a) of title 31;

``(B) reducing or otherwise adjusting apportionments and reapportionments of appropriations for information resources; and

``(C) using other authorized administrative controls over appropriations to restrict the availability of funds for information resources.

``(c) The authorities of the Director under this section (other than the authority described in subsection (b)(6))--

``(1) shall be delegated to the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2);

``(2) shall be delegated to the Secretary of Defense in the case of systems described under subparagraph (C) of section 3532(b)(2) that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense; and

``(3) in the case of all other Federal information systems, may be delegated only to the Deputy Director for Management of the Office of Management and Budget.

``3534. Federal agency responsibilities

``(a) The head of each agency shall--

``(1) be responsible for--

``(A) adequately ensuring the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets;

``(B) developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency; and

``(C) ensuring that the agency's information security plan is practiced throughout the life cycle of each agency system;

``(2) ensure that appropriate senior agency officials are responsible for--

``(A) assessing the information security risks associated with the operations and assets for programs and systems over which such officials have control;

``(B) determining the levels of information security appropriate to protect such operations and assets; and

``(C) periodically testing and evaluating information security controls and techniques;

``(3) delegate to the agency Chief Information Officer established under section 3506, or a comparable official in an agency not covered by such section, the authority to administer all functions under this subchapter including--

``(A) designating a senior agency information security official who shall report to the Chief Information Officer or a comparable official;

``(B) developing and maintaining an agencywide information security program as required under subsection (b);

``(C) ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques;

``(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

``(E) assisting senior agency officials concerning responsibilities

under paragraph (2);
``(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and
``(5) ensure that the agency Chief Information Officer, in coordination with senior agency officials, periodically--
``(A)(i) evaluates the effectiveness of the agency information security program, including testing control techniques; and
``(ii) implements appropriate remedial actions based on that evaluation; and
``(B) reports to the agency head on--

``(i) the results of such tests and evaluations; and

``(ii) the progress of remedial actions.

``(b)(1) Each agency shall develop and implement an agencywide information security program to provide information security for the operations and assets of the agency, including operations and assets provided or managed by another agency.
``(2) Each program under this subsection shall include--

``(A) periodic risk assessments that consider internal and external threats to--
``(i) the integrity, confidentiality, and availability of systems; and

``(ii) data supporting critical operations and assets;

``(B) policies and procedures that--

``(i) are based on the risk assessments required under subparagraph (A) that cost-effectively reduce information security risks to an acceptable level; and
``(ii) ensure compliance with--

``(I) the requirements of this subchapter;

``(II) policies and procedures as may be prescribed by the Director; and
``(III) any other applicable requirements;

``(C) security awareness training to inform personnel of--

``(i) information security risks associated with the activities of personnel; and
``(ii) responsibilities of personnel in complying with agency policies and procedures designed to reduce such risks;
``(D) periodic management testing and evaluation of the effectiveness of information security policies and procedures;
``(E) a process for ensuring remedial action to address any significant deficiencies; and
``(F) procedures for detecting, reporting, and responding to security incidents, including--
``(i) mitigating risks associated with such incidents before substantial damage occurs;
``(ii) notifying and consulting with law enforcement officials and

other offices and authorities;

``(iii) notifying and consulting with an office designated by the Administrator of General Services within the General Services Administration; and

``(iv) notifying and consulting with an office designated by the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President for incidents involving systems described under subparagraphs (A) and (B) of section 3532(b)(2).

``(3) Each program under this subsection is subject to the approval of the Director and is required to be reviewed at least annually by agency program officials in consultation with the Chief Information Officer. In the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), the Director shall delegate approval authority under this paragraph to the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President.

``(c)(1) Each agency shall examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to--

``(A) annual agency budgets;

``(B) information resources management under subchapter I of this chapter;

``(C) performance and results based management under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

``(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 through 2805 of title 39; and

``(E) financial management under--

``(i) chapter 9 of title 31, United States Code, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101 576) (and the amendments made by that Act);

``(ii) the Federal Financial Management Improvement Act of 1996 (31 U.S.C. 3512 note) (and the amendments made by that Act); and

``(iii) the internal controls conducted under section 3512 of title 31.

``(2) Any significant deficiency in a policy, procedure, or practice identified under paragraph (1) shall be reported as a material weakness in reporting required under the applicable provision of law under paragraph (1).

``(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Chief Information Officer, shall include as part of the performance plan required under section 1115 of title 31 a description of--

``(A) the time periods, and

``(B) the resources, including budget, staffing, and training,

which are necessary to implement the program required under subsection (b)(1).

``(2) The description under paragraph (1) shall be based on the risk assessment required under subsection (b)(2)(A).

``3535. Annual independent evaluation

``(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that

agency.
``(2) Each evaluation by an agency under this section shall include--

``(A) testing of the effectiveness of information security control techniques for an appropriate subset of the agency's information systems; and
``(B) an assessment (made on the basis of the results of the testing) of the compliance with--
``(i) the requirements of this subchapter; and

``(ii) related information security policies, procedures, standards, and guidelines.
``(3) The Inspector General or the independent evaluator performing an evaluation under this section may use an audit, evaluation, or report relating to programs or practices of the applicable agency.
``(b)(1)(A) Subject to subparagraph (B), for agencies with Inspectors General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) or any other law, the annual evaluation required under this section or, in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), an audit of the annual evaluation required under this section, shall be performed by the Inspector General or by an independent evaluator, as determined by the Inspector General of the agency.
``(B) For systems described under subparagraphs (A) and (B) of section 3532(b)(2), the evaluation required under this section shall be performed only by an entity designated by the Secretary of Defense, the Director of Central Intelligence, or another agency head as designated by the President.
``(2) For any agency to which paragraph (1) does not apply, the head of the agency shall contract with an independent evaluator to perform the evaluation.
``(c) Each year, not later than the anniversary of the date of the enactment of this subchapter, the applicable agency head shall submit to the Director--
``(1) the results of each evaluation required under this section, other than an evaluation of a system described under subparagraph (A) or (B) of section 3532(b)(2); and
``(2) the results of each audit of an evaluation required under this section of a system described under subparagraph (A) or (B) of section 3532(b)(2).
``(d)(1) The Director shall submit to Congress each year a report summarizing the materials received from agencies pursuant to subsection (c) in that year.
``(2) Evaluations and audits of evaluations of systems under the authority and control of the Director of Central Intelligence and evaluations and audits of evaluation of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available only to the appropriate oversight committees of Congress, in accordance with applicable laws.
``(e) Agencies and evaluators shall take appropriate actions to ensure the protection of information, the disclosure of which may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws.
``3536. Expiration

``This subchapter shall not be in effect after the date that is two

years after the date on which this subchapter takes effect.".

SEC. 1062. RESPONSIBILITIES OF CERTAIN AGENCIES.

(a) Department of Commerce.--Notwithstanding section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g 3) and except as provided under subsection (b), the Secretary of Commerce, through the National Institute of Standards and Technology and with technical assistance from the National Security Agency, as required or when requested, shall--

(1) develop, issue, review, and update standards and guidance for the security of Federal information systems, including development of methods and techniques for security systems and validation programs;

(2) develop, issue, review, and update guidelines for training in computer security awareness and accepted computer security practices, with assistance from the Office of Personnel Management;

(3) provide agencies with guidance for security planning to assist in the development of applications and system security plans for such agencies;

(4) provide guidance and assistance to agencies concerning cost-effective controls when interconnecting with other systems; and

(5) evaluate information technologies to assess security vulnerabilities and alert Federal agencies of such vulnerabilities as soon as those vulnerabilities are known.

(b) Department of Defense and the Intelligence Community.--

(1) In general.--Notwithstanding any other provision of this subtitle (including any amendment made by this subtitle)--

(A) the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President, shall, consistent with their respective authorities--

(i) develop and issue information security policies, standards, and guidelines for systems described under subparagraphs (A) and (B) of section 3532(b)(2) of title 44, United States Code (as added by section 1061 of this Act), that provide more stringent protection, to the maximum extent practicable, than the policies, principles, standards, and guidelines required under section 353 of such title (as added by such section 1061); and

(ii) ensure the implementation of the information security policies, principles, standards, and guidelines described under clause (i); and

(B) the Secretary of Defense shall, consistent with his authority--

(i) develop and issue information security policies, standards, and guidelines for systems described under subparagraph (C) of section 3532(b)(2) of title 44, United States Code (as added by section 1061 of this Act), that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that provide more stringent protection, to the maximum extent practicable, than the policies, principles, standards, and guidelines required under section 3533 of such title (as added by such section 1061); and

(ii) ensure the implementation of the information security policies, principles, standards, and guidelines described under clause (i).

(2) Measures addressed.--The policies, principles, standards, and guidelines developed by the Secretary of Defense and the Director of Central Intelligence under paragraph (1) shall address the full range of information assurance measures needed to protect and defend Federal

information and information systems by ensuring their integrity, confidentiality, authenticity, availability, and nonrepudiation.

(c) Department of Justice.--The Attorney General shall review and update guidance to agencies on--

(1) legal remedies regarding security incidents and ways to report to and work with law enforcement agencies concerning such incidents; and

(2) lawful uses of security techniques and technologies.

(d) General Services Administration.--The Administrator of General Services shall--

(1) review and update General Services Administration guidance to agencies on addressing security considerations when acquiring information technology; and

(2) assist agencies in--

(A) fulfilling agency responsibilities under section 3534(b)(2)(F) of title 44, United States Code (as added by section 1061 of this Act); and

(B) the acquisition of cost-effective security products, services, and incident response capabilities.

(e) Office of Personnel Management.--The Director of the Office of Personnel Management shall--

(1) review and update Office of Personnel Management regulations concerning computer security training for Federal civilian employees;

(2) assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and computer security best practices; and

(3) work with the National Science Foundation and other agencies on personnel and training initiatives (including scholarships and fellowships, as authorized by law) as necessary to ensure that the Federal Government--

(A) has adequate sources of continuing information security education and training available for employees; and

(B) has an adequate supply of qualified information security professionals to meet agency needs.

(f) Information Security Policies, Principles, Standards, and Guidelines.--

(1) Adoption of policies, principles, standards, and guidelines of other agencies.--The policies, principles, standards, and guidelines developed under subsection (b) by the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President may be adopted, to the extent that such policies are consistent with policies and guidance developed by the Director of the Office of Management and Budget and the Secretary of Commerce--

(A) by the Director of the Office of Management and Budget, as appropriate, for application to the mission critical systems of all agencies; or

(B) by an agency head, as appropriate, for application to the mission critical systems of that agency.

(2) Development of more stringent policies, principles, standards, and guidelines.--To the extent that such policies are consistent with policies and guidance developed by the Director of the Office of Management and Budget and the Secretary of Commerce, an agency may develop and implement information security policies, principles, standards, and guidelines that provide more stringent protection than

those required under section 3533 of title 44, United States Code (as added by section 1061 of this Act), or subsection (a) of this section.

(g) Atomic Energy Act of 1954.--Nothing in this subtitle (including any amendment made by this subtitle) shall supersede any requirement made by, or under, the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted Data or Formerly Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SEC. 1063. RELATIONSHIP OF DEFENSE INFORMATION ASSURANCE PROGRAM TO GOVERNMENT-WIDE INFORMATION SECURITY PROGRAM.

(a) Consistency of Requirements.--Subsection (b) of section 2224 of title 10, United States Code, is amended--

(1) by striking ``(b) Objectives of the Program.--" and inserting ``(b) Objectives and Minimum Requirements.--(1)"; and

(2) by adding at the end the following:

``(2) The program shall at a minimum meet the requirements of sections 3534 and 3535 of title 44.".

(b) Addition to Annual Report.--Subsection (e) of such section is amended by adding at the end the following new paragraph:

``(7) A summary of the actions taken in the administration of sections 3534 and 3535 of title 44 within the Department of Defense.".

SEC. 1064. TECHNICAL AND CONFORMING AMENDMENTS.

(a) Table of Sections.--Chapter 35 of title 44, United States Code, is amended--

(1) in the table of sections--

(A) by inserting after the chapter heading the following:

``SUBCHAPTER I--FEDERAL INFORMATION POLICY";

and

(B) by inserting after the item relating to section 3520 the following:

``SUBCHAPTER II--INFORMATION SECURITY

``Sec.

``3531. Purposes.

``3532. Definitions.

``3533. Authority and functions of the Director.

``3534. Federal agency responsibilities.

``3535. Annual independent evaluation.

``3536. Expiration.";

and

(2) by inserting before section 3501 the following:

``SUBCHAPTER I--FEDERAL INFORMATION POLICY".

(b) References to Chapter 35 .--Sections 3501 through 3520 of title 44, United States Code, are amended by striking ``chapter" each place it appears and inserting ``subchapter", except in section 3507(i)(1) of such title.

SEC. 1065. EFFECTIVE DATE.

This subtitle and the amendments made by this subtitle shall take effect 30 days after the date of enactment of this Act.